Description

Procedure to Increase the Security of Authentication Processes in Digital Mobile Radio Systems

The invention concerns a procedure for the increased security of authentication processes for digital mobile radio system, according to the characterizing clause of patent claim 1.

Modern mobile radio networks have special security features and precautions, which prevent unauthorized use of operating equipment or resources by anyone other than authorized persons and protects against possible eavesdropping or tapping of radio operations. The security measures refer, therefore, to the protection of the relationship between the mobile radio network and the authorized user. A special procedure for authorizing the user will prevent a third party from stealing the authorized user's identity. By comparing his subscriber identification module with the stored data and functions in the mobile radio network, a user must be authenticated. In the past, it has been shown over and over that authentication processes can be compromised (i.e. spying on the subscriber's secret code KI) with specialized knowledge and the right equipment, and that this is possible by sequencing random numbers and response numbers (that is, RAND / SRES pairs) that can be subjected in larger quantities to mathematical procedures, in order to determine the secret code KI of a user. Once the secret code KI has been determined, an illegal duplication of the subscriber's identification module is possible.

With the authentication processes currently being used, the mobile radio network uses special algorithms and a SIM-specific secret code KI from a random value RAND for an authentication result SRES and a temporary code KC. In this way, the mobile radio network has a certain number of RAND/SRES/KC-triplets. If a user want to sign in, the mobile radio network transmits a random number RAND to the subscriber's identification module SIM. The SIM determines, with the same special algorithms and its SIM-specific secret code KI, a corresponding SRES/KC-pair and send the determined SRES back to the mobile radio network. The mobile radio network compares the received SRES with the previously held SRES to see if they conform so that a match authenticates the subscriber. The code KC is calculated and evaluated on both sides to encode the transmission.

As previously stated, with the procedures currently being used, it is possible to compromise or spy on the code KI in order to gain unauthorized access to the mobile radio network.

The present invention is based on the task of improving the security of the authentication procedures of digital mobile radio systems, which make it nearly impossible to discover the secret codes.

The characterizing features in patent claim 1 solve the task.

The invention is based, thus, on the fact that there are several various secret SIM-specific codes KI stored in the subscriber's identification module in the mobile radio network and selects a code from several pre-held secret codes for the completion of the authentication between the subscriber's identification module and the mobile radio network.

The advantage of this procedure is based on the fact that a compromise (i.e. spying or ferreting out the secret code KI) of the SIM is made substantially more difficult because it is not foreseeable nor discernable to the "aggressor" or "attacker" which secret code KI of the SIM is being used to calculate the SRES answer.

Another essential advantage of this procedure is that a modification to the (interface) operations of the mobile radio network, in particular the air operations (interface) is not necessary. Likewise, no modification at the terminals or end equipment must be made. Only local software-technical modifications at individual network components of the mobile radio network, as well as on the SIM, are necessary and these are feasible without hardly any costs and very little expenditure.

Advantageously, the selection of used codes KI result from the SIM according to the random principle.

In a preferred embodiment, the mobile radio network determines with special algorithms under specifications, respectively, a SRES/KC-pair from random number RAND for all SIM-specific codes KI of a user, and forms the so-called RAND/SRES/KC-triplets with the respectively used RAND. The triplet is held in the mobile radio network and can be called upon for future authentication procedures.

For starting up an authentication, the mobile radio network transmits a random value RAND of one of these triplets to the subscriber identification module SIM, and then, the subscriber identification module selects an available code on the basis of the transmitted RAND and calculates the appropriate values for the SRES response and the code KC on the basis of this selected code KI and sends back the SRES response to the mobile radio network.

In the mobile radio network, a comparison now takes place to determine the conformity or matching of the received response SRES to all the SRES values held for the used RAND so that if a match is met between two user specific responses SRES, the user's authentication is validated.

Preferably, the mobile radio network will now use the corresponding SRES belonging to the KC to encode the transfer or transmission so that the identical code KC is available in the SIM and is also used for the encoding of the transmission.

Subsequently, an embodiment of the invention is explained more closely in a drawing representation. Further characteristics, features and advantages of the invention are shown in the drawing and corresponding description.

Figure 1 shows an authentication procedure in a simplified representation according to the invention. In order to complete the procedure, several secret codes KI must be stored for each user in the mobile radio network and, also, in the subscriber identification module.

Mobile radio network: User X

	KI 1	KI 2	KI 3
RAND 1	SRES/KC (1,1)	SRES/KC (1,2)	SRES/KC (1,3)
RAND 2	SRES/KC (2,1)	SRES/KC (2,2)	SRES/KC (2,3)
RAND 3	SRES/KC (3,1)	SRES/KC (3,2)	SRES/KC (3,3)
...	...	...	...

As shown in the table above, for example, three secret codes KI are set aside in the mobile radio network for each subscriber X so that now the mobile radio network has settings of several random numbers RAND 1, RAND 2 and RAND 3 and, in each case, secret codes KI 1, KI 2 and KI 3 that calculate and store corresponding SRES responses and codes KC.

Also in the subscriber identification module for the subscriber or user X, three possible codes KI 1, KI 2 and KI 3 are set aside.

If the user want to check into the mobile radio network, the authentication procedures must first be completed, as is shown in figure 1. The subscriber identification module first transmits the subscriber identity number IMSI over an appropriate terminal or end device to the mobile radio network. If this IMSI is recognized as admissible, then the mobile radio network chooses a random value from a stored random value RAND for the user X (here, for example, RAND 3) and sends this back to the subscriber identification module. The subscriber identification module selects again one of the user specific secret codes KI (for example, KI 2) and from the RAND 3 and the KI 2, calculates the corresponding SRES response and the code KC received by the mobile radio network. The SRES response, that was formed from the code KI 2 and the RAND 3, is transmitted back to the mobile radio network and compared with the stored SRES value to KI 2 and RAND 3. If these SRES values correspond, then the user is considered authenticated and can check into mobile radio network. The available codes KC are utilized on both sides during the newly-made connection to encode the data communication.